IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

IIROC NOTICE

Education Notice
Guidance Notice

Please distribute internally to:
Corporate Finance
Credit
Institutional
Internal Audit
Legal and Compliance
Operations
Registration
Regulatory Accounting
Research
Retail
Senior Management
Technology & Cybersecurity
Trading Desk
Training

Contact:
Suzanne Lasrado
Senior Manager, Financial & Operations Compliance
416-943-5880
slasrado@iiroc.ca

Ryan Li
Director, Information Security
416-943-5890
rli@iiroc.ca

20-0235
November 9, 2020

Cybersecurity and Fraud – Protecting Clients

This Notice outlines the types of cybersecurity and fraud attacks that target clients of the firm but may not necessarily represent an attack on the firm. It discusses what firms and advisors can do to prevent or limit the loss of client information and/or assets, and what you should do if a client's information or assets held at your firm has been compromised or stolen. The Notice also summarizes when and how to report such incidents to IIROC.

Overview

In previous Notices, IIROC focused on what firms and advisors should do to protect clients and itself from an attack on the firm. However, clients can also become victims of fraud and identity theft as a result of attacks that have occurred from outside the firm. Many times, a compromised client may not be aware that their personal or login information was stolen.

Cyber attackers and fraudsters seek to harm the client by using fraudulently obtained information about the client to conduct unauthorized trades in, or steal information or assets from the client account at the firm. Firms and advisors should remain vigilant to prevent client loss and harm from such attacks. Accordingly, firms should strongly consider implementing controls to try to minimize the impact on and risk of loss to these compromised clients.

Types of incidents and attacks

These are some of the ways we've seen compromised clients being attacked at our firms:

Social engineering attacks

A malicious actor can deceive an advisor or an employee of the firm into sharing sensitive client information, transferring client funds, or conducting unauthorized trades in the client account by presenting themselves as the client or someone authorized to act on behalf of the client. These attacks can involve several different media including but not limited to email, phone calls, text messages and messenger services.

Fraudulent account openings and account intrusions

An attacker can use fraudulently obtained personal information about the client to:

- create an account for the client at the firm, and even fund the account from fraudulently obtained banking information in order to conduct unauthorized trades
- hack into an existing client's account at the firm and steal assets or conduct unauthorized trades in the account.

Online trading divisions and Order Execution Only (**OEO**) firms should be on guard for such incidents. Given the increase in pandemic-related cybersecurity attacks and the significant increase in account openings since the pandemic began, OEO firms are strongly advised to remain extra vigilant and cautious to such incidents.

Credential stuffing

This is a type of cyberattack where stolen login credentials are used to gain unauthorized access to client accounts through automated login requests against the firm's online applications. These login credentials were typically included in lists of usernames and passwords that were most likely stolen from a data breach that occurred elsewhere. Since many people tend to use the same combination of username and passwords across different websites and applications, these types of attacks can often be successfully used to hack into the client's account at the firm.

Recommended protection, identification and detection controls

Firms should establish controls to prevent and identify attacks on clients which include but are not limited to:

1) **Implementing firm-level controls, policies and procedures** that should, at a minimum,
    - Require the firm to independently verify client identity particularly when opening accounts electronically[1]
    - Require the client to independently verify requests for sensitive client information or orders in unusual or large trades
    - Establish hold periods and require additional firm approval and client verification to transfer out assets that exceed certain established limits
    - Establish processes to:
        - respond expeditiously to client complaints, calls and inquiries about unusual account activity, account intrusions and misappropriation of assets
        - quickly investigate a suspected intrusion, unauthorized activity or loss of assets from a client account to determine the root cause and extent of the attack.

2) Setting up **online client accounts with strong authentication** controls
    - Implement multi-factor authentication
    - Set up conditional access rules and CAPTCHA[2]
    - Require strong passwords and frequent changes

3) **Educating advisors** to exercise caution when dealing with requests from clients

---

[1] Firms' policies must ensure compliance with Anti-Money Laundering legislation and regulation governing non face-to-face verification of identification documents.

[2] CAPTCHA or "Completely Automated Public Turing test to tell Computers and Humans Apart" is a response test challenge used to determine whether the online account login request is coming from a person or a computer.

- Be extra vigilant when dealing with requests that pertain to transferring assets out of the account
- Consider whether the request from the client seems unusual and accordingly, verify the request using information that only the advisor and client would know:
  - Is this a normal course request from the client?
  - Was the request made through a channel and in a manner that the client normally uses to communicate with the firm?
  - Does the request feel suspicious in any way?
- Be familiar with the firm's response protocols when an unusual client request comes in, or if a possible unauthorized account intrusion is suspected

4) **Monitoring for anomalous behaviour** to mitigate the impacts of fraud or a cyber-attack
   - Monitor real-time alerts and post-trade compliance reviews to detect abnormal deviations from a client's normal trading patterns
   - Monitor for abnormal deviations in login requests or activity
   - Block access to a client account or require further authentication if an unrecognized IP address is used
   - Monitor lists of known fraudulent IP addresses and block access by such addresses to the firm's systems

5) **Educating clients** on how to protect themselves from online fraud and what to do if they suspect they have been compromised
   - Advise them
     - not to share login credentials or personal identification information with anyone or any application or website unless they have personally and independently verified the request
     - not to use public wireless networks
     - to set up multi-factor authentication
     - to create strong passwords
     - to notify the firm if they suspect they are a victim of identity theft or fraud
   - Provide clear instructions and contact information to clients on how to notify the firm if they notice unusual activity, suspect a breach of, unauthorized trading in or stolen assets from their account at the firm
   - Provide information to clients on their rights under various federal and provincial laws and how to file complaints with the relevant authorities

6) **Providing other free services or resources** to clients
   - Webinars and educational material on cybersecurity threats and alerts
   - Downloads of anti-virus, anti-spyware and anti-malware software for clients to install on their computers to provide extra protection
   - Secure applications to generate and store passwords

Recommended recovery and response controls

Firms should implement controls to respond to attacks on clients which include but are not limited to:

1) **Notifying the affected client(s)** that they have been compromised and advising them to
    - change their login credentials at the firm and at other websites as well
    - get a credit bureau report

2) **Taking remedial action to protect the account** including suspending accounts and requiring clients to set new passwords or create new accounts

3) **Contacting the banking institution** to stop the transfer of funds, if applicable

4) **Investigating the incident** to determine the scope and extent of the attack (even if it appears to be isolated to an individual client) in order to verify that the incident
    - was not an attack on the firm
    - did not occur due to a failing on the part of the firm or an employee of the firm
    - does not result in contagion or impact to other clients.

5) **Reporting the incident to the applicable authorities**, commissioners, regulators and IIROC. For more information on reporting to IIROC, see the section below.

Report the incident to IIROC

1) If the incident meets the requirements of IIROC Rule 3100(B.1.1) ***Cybersecurity Reporting***, then firms must contact their IIROC Financial & Operations Compliance manager to provide the required information.

2) Any **internal investigations by the firm or complaints received from clients** in relation to these incidents that meet the requirements of IIROC Rule 3100 must be reported on ComSet.

3) If the firm suspects or has reason to believe that there was **unauthorized trading activity** in a client's account, we ask that firms report these incidents as "account intrusions" to IIROC. Participants and Access Persons can file a report in the Gatekeeper system through the IIROC Services Portal.

4) Please provide information about **other incidents** to IIROC at CyberIncidents@iiroc.ca

Other resources

Further information and resources on managing cybersecurity threats, including guides and webinars, are available on IIROC's cybersecurity site.